
VONAGE
Part of Ericsson

VONAGE DATA SECURITY AND PROTECTION POLICY

Last updated October 16, 2024

v 3.0

The Vonage Data Security and Protection Policy (this "Policy") is designed to protect Vonage Data in all situations and wherever they are located. This Policy is intended to protect the confidentiality of all Vonage Data, including corporate, employee, vendor, partner, and customer information. Supplier has specific obligations with regard to the protection of Vonage Data. Supplier shall process Vonage Data only in accordance with the Agreement, this Exhibit, written instructions by Vonage, and any model contracts executed by the Parties.

1. DEFINITIONS

a. "Applicable Data Protection Laws" mean certain local, state, and federal laws, and international regulations, regulatory frameworks, or other legislations relating to the processing and use of Personal Data, as applicable to Vonage's use of the Service and the provision of the Service by Supplier, including (a) the EU General Data Protection Regulation 2016/679 ("GDPR"), along with any implementing or corresponding equivalent national laws or regulations, once in effect and applicable; and (b) the U.S. Department of Commerce and European Commission's EU--U.S. Privacy Shield Framework ("Privacy Shield"), or any succeeding legislation, available at https://www.privacyshield.gov/, or any succeeding URL, as may be amended.

b. "GDPR" means the EU General Data Protection Regulation 2016/679.

c. "Personal Data" means any data relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, or located directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person,

d. "Process", "Processed" or "Processing" means anything that is done to or with Vonage Data, including but not limited to collection, transmittal, viewing, creation, compilation,

use, access, disclosure, storage, combination, alteration, erasure, or destruction.

e. "Security Breach" means a confirmed or reasonably suspected (i) a breach of Personal Data or (ii) the intentional or unintentional release of Vonage Data to an individual or organization not authorized to Process such information.

f. "Sensitive Information" means information which is part of Vonage Data, which due to its nature has been classified by law or regulation, as requiring additional privacy and security protection or where no such laws apply, means an individual's financial information (including financial account information and/or payment card industry data), sexual preferences, medical or health information, and personal information of children protected under any child protection laws (such as the personal information defined under the U.S. Children's Online Privacy Protection Act).

g. "Subprocessor" means any third party (including an Affiliate of Supplier) that provides services to Supplier and that may have access to encrypted Vonage Data.

h. "Transfer" means to disclose or make available Vonage Data to a third party, including a Supplier Affiliate or one of its Subprocessor, either by physical movement of Vonage Data to such third party or by enabling access to Vonage Data.

i. "Vonage Data" means, collectively, all Vonage Confidential Information, Personal Information, and/or Sensitive Information processed by Supplier in connection with any Agreement in place between Vonage and Supplier.

2. GENERAL OBLIGATIONS

a. Compliance with Laws. Supplier represents that it shall comply with Applicable Data Protection Laws to the extent applicable to Supplier Processing or Transferring of Vonage Data. Supplier also agrees to comply with its own privacy and security policies.

b. Internal Security Policy. Supplier has, or agrees to implement, an internal security policy governing the protection of its own information technology and the resources of others under its control. Such policy shall be subject to Vonage's review upon written request by Vonage. A copy of Supplier's security policy shall be made available upon request.

c. Protected Health Information. If the Vonage Data includes protected health information as defined in the HIPAA Privacy and Security Rules, the parties shall execute a Business Associate Agreement.

d. Breach. Failure to comply with the provisions of this Policy is considered a material breach under the Agreement.

e. Termination. When Supplier ceases to perform Services for Vonage, Supplier will return or destroy Vonage Data, unless prevented. Electronic media containing Vonage Data will be disposed of in a manner that renders it unrecoverable. If Supplier is required by applicable data protection laws or audit requirements to retain any Vonage Data, Supplier warrants that it shall (i) ensure the continued confidentiality and security of Vonage Data; (ii) delete or destroy Vonage Data when the retention period expires; and (iii) not actively process Vonage Data other than as needed to comply with its requirements.

3. SECURITY AND AUDIT OBLIGATIONS

a. Security Reviews. Supplier shall submit and update annually, when requested by Vonage, a security questionnaire for Vonage to review the Supplier's compliance with this Policy. Supplier's responses shall be accurate and complete at all times.

b. Security Measures. Supplier shall ensure that all industry standard security measures current at the time of Processing are in place to protect Vonage Data, including physical, technical, and administrative safeguards and controls to protect Vonage Data against accidental, unauthorized, or unlawful Processing or Transfer, alteration, loss, disclosure or destruction. This includes any records made for quality assurance. Such protections shall include, but not be limited to, (a) protecting against virus, malware and other Supplier side intrusions; (b) encrypting Personal Data and Sensitive Information in transmission and in storage; (c) protecting against intrusions of operating systems or software; and (d) have industry standard Account and Access Management procedures in place that are designed and implemented with a mechanism that will prevent unauditable and unauthorized access.

c. Authorized Use. Supplier shall only Process or Transfer Vonage Data as necessary to perform the Services and as authorized pursuant to an Order, SOW, or a DPA. It will not sell, share, or otherwise transfer or disclose any Vonage Data received from Vonage to any other party without prior written consent from Vonage.

d. Access to Information. Supplier shall ensure that only persons with a need to know are allowed to access Vonage Data, and only to and for the limited extent and purpose for which such persons have a need to know. All parties who have access to Vonage Data must be bound by legally enforceable confidentiality obligations similar to those contained in the Confidential Information section of this Agreement.

e. Network Security. If the Processing involves the transmission of Vonage Data over a network, Supplier shall have implemented appropriate supplementary measures to protect

the Vonage Data against the specific risks presented by the Processing. The transmission of Vonage Data must utilize FIPS 140-2 compliant secure transmission protocol and data encryption (both in transit and at rest). Firewalls shall be configured according to industry best practices

f. Data Center Physical Safeguards. Supplier and its Subprocessors shall comply with physical security controls outlined in industry standards, and that possess a valid annual external audit certification report, such as SOC 2 or ISO 27001 certifications. Supplier must maintain such certifications for the duration of this agreement. Only allow Personnel with business critical need to know to have access to controlled access areas.

g. Access Points. Any externally facing web servers and third-party access points will be configured securely to include, but not be limited to, employing only FIPS 140-2 compliant secure transmission and data encryption protocols.

h. Encryption. Supplier shall encrypt Vonage Data using FIPS 140-2 compliant encryption protocols.

i. Monitoring. Supplier shall regularly monitor the security of its network to (i) identify patterns of suspicious network activity; (ii) transaction activity that might indicate unusual transaction types, volumes, timing, or amounts violations or attempts; and (iii) login violations or attempts.

j. Testing. Supplier shall regularly test and monitor the effectiveness of its safeguards, controls, systems, and procedures. Testing should include annual network penetration testing.

k. Portable Devices. Vonage Data may not be stored on portable computer devices or media including, without limitation, laptop computers, removable disks, USB or flash drives, mobile phones, or CDs.

l. Business Continuity/Disaster Recovery. Supplier shall have documented business continuity and disaster recovery plans to enable it to continue to provide the Services in a timely manner in the event of business interruption. Supplier will regularly test and monitor the effectiveness of such plans and provide confirmation of such tests at Vonage's written request.

m. Destruction of Information. Unless otherwise required by law, upon termination or cancellation of the Agreement or a relevant Order or SOW, or at Vonage's written request, all Vonage Data (including media used to transmit data and to create backups of Vonage Data) must be (a) destroyed in a manner that causes all Vonage Data to be irrecoverable and/or; (b) returned to Vonage upon completion of the Services in a manner acceptable to Vonage; and (c) certify in writing that all Vonage Data has been returned to or destroyed after its use, or as agreed.

n. ISO/IEC and PCI Compliance. Supplier and/or its

Subprocessor who will be creating, handling, modifying, storing, processing, accessing, transferring or interacting with credit card data for Vonage customers in any form, agrees that it is responsible for ensuring the protection and preventing the unauthorized disclosure or use of such data. Further, Supplier represents that it currently conforms, and warrants that it will continue to comply at all times during the Agreement, with the standards of the Payment Card Industry ("PCI") for information security, and shall provide to Vonage promptly, upon request from time to time as considered necessary by Vonage, valid proof of certification by a recognized certifying organization. The current standards may be found at http://www.pcisecuritystandards.org. Without limiting Vonage's other remedies, Supplier agrees to be responsible for any and all fines or penalties incurred by Vonage on account of any PCI violation by Supplier or its Affiliates or Subprocessors provided that such fines or penalties would not have been incurred but for Supplier violation and provided that Supplier's liability shall be limited with respect to that portion of such fines or penalties as is equivalent to the proportion of Supplier's violation relative to all other causes of such claims as determined by a root cause analysis of the causes. Where there is a conflict between the standards used by ISO/IEC and PCI, the most current PCI standard shall govern.

o. Security Updates and Reviews. Supplier shall implement security changes, patches, and upgrades in networks, systems, applications, and software in a timely manner and commensurate with the threat to Vonage Data but no later than ninety (90) days from release, or in accordance with Supplier's Patch and/or Vulnerability Management policy. Security changes, patches, and upgrades correcting significant or immediate security issues shall be implemented immediately, subject to appropriate testing, no later than ten (10) days after release, or in accordance with Supplier's Patch and/or Vulnerability Management policy.

p. Service Organization Control Reports. If Supplier will be creating, handling, modifying, storing, processing, accessing, transferring, or interacting with Vonage Data, Supplier will execute, at its own expense, external, independent audits to produce a SOC-2 audit report or any successor report thereto. Supplier will continue to execute audits and issue corresponding reports for the duration of the Agreement on at least an annual basis. In addition, if requested by Vonage, Supplier shall deliver to Vonage a letter from a senior executive of Supplier that: (i) contains a written representation that Supplier's internal controls as represented in the most recent SOC-2 audit report remains in all material respects unchanged through the date of the letter; or (ii) identifies all material changes in Supplier's internal controls since the most recent SOC-2 audit report.

q. Due Diligence over Personnel and Subprocessors.

Supplier shall maintain appropriate due diligence when utilizing Supplier personnel or Subprocessors who may have access to Vonage Data.

r. Security Awareness Training. Supplier will, at least annually, conduct security awareness and privacy training for its personnel that is appropriate to the job functions of such personnel.

4. AUTHORIZED TRANSFER

a. Subprocessors. Supplier shall not Transfer Vonage Data without the prior written consent of Vonage. Supplier shall be liable for Transfers of Vonage Data to its Subprocessors. Supplier shall ensure that Subprocessors are contractually bound to comply with or provide at least the same level of confidentiality, security, and privacy protection as is required of Subprocessors by the Privacy Shield Principles and the Applicable Data Protection Laws and the terms of this Exhibit. Supplier shall provide Vonage a list of all Subprocessors within five (5) business days of any request.

b. International Transfers. Supplier shall not Transfer Vonage Data across national borders or permit remote access to Vonage Data from any Subprocessor or other third party outside the country in which the Vonage Data originated unless Supplier has the prior written consent of Supplier for such Transfer. Supplier agrees that Vonage must authorize all cross-border transfers, including by use of approved Transfer mechanisms.

5. SECURITY BREACH

a. Notification. If Supplier discovers or is notified of a Security Breach or which is related to any fraudulent or unauthorized use of Vonage Data, Supplier shall notify Vonage within 72 hours upon discovery of a Security Breach and fully cooperate with the investigation and remediation, up to and including prosecution of involved individuals. This notification must be made via email to Vendor.Security@vonage.com. Supplier shall have incident management policies and procedures in place to handle a Security Breach

b. Remediation. Supplier shall be fully responsible for all damages, fines (whether criminal or civil) and costs arising from a Security Breach arising from either (i) the negligence or misconduct of Supplier or any Subprocessor or (ii) the failure of Supplier to comply with the terms of the Agreement. Any failure of Supplier to abide by, train its personnel on, or enforce any of the terms contained in this exhibit will be considered a material breach of the Agreement.

6. CFIUS RESTRICTIONS

As a result of Ericsson's acquisition of Vonage, there are government requirements and restrictions that Vonage must adhere to. These requirements and restrictions are mandated by the Committee on Foreign Investments in the United States ("CFIUS"). The location where Vonage data can be stored, the countries where originates from, and who can access the data fall into the CFIUS requirements and restrictions. Suppliers will be presented with the appropriate version of contractual language based on the type of engagement for their awareness and agreement.

2.12.2024, 04:53:55

Thu Jun 26 2025 18:58:42 GMT+0200 (Mitteleuropäische Sommerzeit)